Smart Cards: State-of-the-Art to Future Directions

(Invited Paper)

Raja Naeem Akram
Cyber Security Lab, Department of Computer Science
University of Waikato, Hamilton.
New Zealand.
Email: rnakram@waikato.ac.nz

Konstantinos Markantonakis
Smart Card Centre: Information Security Group
Royal Holloway, University of London.
Egham, United Kingdom
Email: {k.markantonakis}@rhul.ac.uk

***Abstract*—The evolution of smart card technology provides an interesting case study of the relationship and interactions between security and business requirements. This paper maps out the milestones for smart card technology, discussing at each step the opportunities and challenges. The paper reviews recently proposed innovative ownership/management models and the security challenges associated with them. The paper concludes with a discussion of possible future directions for the technology, and the challenges these present.**

***Keywords*-Smart Card, Java Card, Multos, GlobalPlatform, Issuer Centric, Consumer-Centric, User Centric.**

I. Introduction

Smart cards are the most widely deployed tamper-resistant secure devices [1]. It is difficult to envisage performing the mundane tasks of modern life without smart cards. A range of private and governmental organisations have played an important role in the development, promotion, and wide-scale deployment of smart cards.

Smart card technology has enabled diverse organisations, referred to as "Service Providers (SPs)", to provide secure services to their consumers. Along with their strong security properties, the cards are very convenient for end users and come at a reasonable cost to individual Service Providers (SPs). The SPs not only get a secure product at modest expense, but they can also use the card body for brand exposure.

Technology sometimes evolves to support certain business requirements, whereas on other occasions, technical innovations appear that then need applications to exploit them. Success is not always assured and an innovation may not catch on, either because of difficulties with business models or because it exceeds the requirements of the time [2]. Smart card technology is no different: it has its success stories along with excellent innovations that did not catch on.

This paper explores different milestones in the smart card's technological evolution and evaluates the successes and failures. Finally, the current opportunities and challenges faced by smart card technology are considered.

A. Structure of the Paper

Section II presents a succinct history of smart card technology. Section III discusses the proposed security models for smart card technology. In section IV, the current trends in the smart card industry are discussed along with the challenges and opportunities. In section V, possible future directions are explored along with how these might change the overall architecture of smart card technology. Conclusions are presented in section VI.

II. Smart Card Evolution

This section explores the evolution of smart card platforms from a single application platform to a feature-rich multiapplication platform.

A. Monoapplication Smart Cards

Early smart cards only supported a single application. The application represented the services provided by the SP, who acquired these cards from the card manufacturer and issued them to their respective consumers. In this model, referred as "Issuer Centric Smart Card Ownership Model (ICOM)", SPs buy the cards and in most instances give them to the consumers (i.e. card users) free of cost.

Early monoapplication smart cards required the development of the respective applications functionality as part of the Smart Card Operating System (SCOS). The first monoapplication smart cards were based on Monolithic SCOSs in which applications were closely tied up with the SCOS code [3]. This model required that the application developers have in-depth understanding of how the SCOS worked.

Later, another concept termed the "generic soft mask" [4] took centre stage. In the generic soft mask, a card manufacturer implements a Smart Card Operating System (SCOS) on a non-mutable memory on the smart card. This operating system is independent of installed applications like banking or transport. To support these applications, the card manufacturer implements Application Programming Interfaces (APIs) to facilitate the requirements of individual applications. These APIs are stored on a mutable memory rather than on a non-mutable memory where traditionally the bulk of the SCOS was stored. This innovation simplified the development of smart card applications: card manufacturers proposed using generic soft masks for different types of applications. Implementing the concept of the generic soft mask requires a minimum operating system and some customized Application Programming Interfaces (APIs) for any particular application.

The introduction of the soft mask also enabled smart card developers to have a single smart card which had multiple applications. These were fundamentally different from multi-functional smart cards because each of the functionalities/services had a separate application in the smart card. One example of an initial soft mask-based multiple application smart card is the French banking card. It had the old B0' application [5], EMV [6] banking application and a French (electronic) purse called Moneo [7], [8]. When a smart card user presented his/her smart card at a terminal, the card first checked whether or not the terminal supported EMV. If it did not, then it could opt for the B0' French banking application. Although these smart cards had separate functional applications, we cannot term them true multiapplication smart cards because of the rigidity of their architecture. Once these smart cards were issued, not even the card issuers (i.e. SPs that issue smart cards) could update them or install new applications.

B. Multiapplication Smart Cards

Multiapplication smart cards support the features listed below [1], [4], [9], [10]:

1) A separate context for each application on the card (e.g. storage and execution isolation), ensuring a secure and reliable application segregation mechanism.
2) Post-issuance application installation, deletion, and management (update/modification).
3) The ability for terminals to select an application directly and independently of other on-card applications.
4) The management, updating, modification, and deletion of each application without affecting other applications.
5) Delegation of the management of an application to an entity, which is not necessarily the card issuer. If an application is managed by such an entity, then the card issuer cannot access the application context. The only possible authority a card issuer might have is to block and/or remove the application without accessing its contents.
6) Secure and reliable inter-application communication.

A large number of smart cards deployed today are single task devices which can only execute one application at a time, and do not support the simultaneous execution of multiple applications. However, innovations in hardware design and in the SCOS/platforms have begun to explore the concept of multi-threading [11]. These developments will surely make smart cards into powerful and secure computing devices which can support different tasks concurrently.

The two main de-facto standards of multiapplication smart cards are Java Card [11] and Multos [12], which are discussed in subsequent sections. In addition, no discussion on multiapplication smart cards can be complete without discussing the GlobalPlatform [13] specification as presented in section II-B3.

1) MULTOS: In 1997, a consortium of companies (MAOSCO) supported the development of an SCOS called Multos [12], with one aim: to provide a high level of security and reliability. They required a single operating system which could be implemented on any silicon chip and which had an application written for it that was independent of the underlying hardware. Their vision anticipated the creation of a multiapplication smart card. From the beginning, Multos was developed as a secure multiapplication SCOS that achieved ITSEC[1] Assurance Level E6 [15] (comparable to the Common Criteria EAL7 [16], [17]), which is the highest level attained by any SCOS [1].

The Multos card architecture is illustrated in Figure 1. At the top in Figure 1 is the application layer, which contains three applications (namely A, B, and C); each application has its own space, which is protected by the card's firewall mechanism. The next layer is the Application Abstract Machine (AAM), which also includes different APIs. The Multos operating system presides over the hardware and provides services such as communication, memory management, the handling of loading and deleting of applications, together with APDU commands and responses. At the bottom of the figure is the hardware, which supports the SCOS. Functions that access this layer are written in native language, but are accessed by a fully specified virtual machine, which is the same no matter what the hardware.

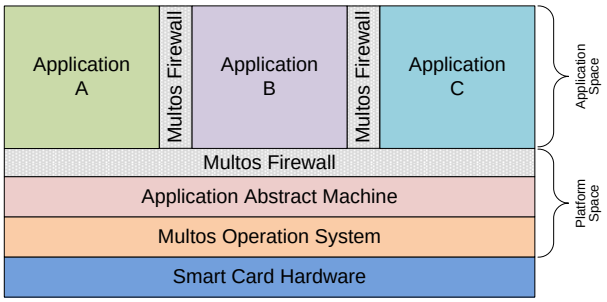

Fig. 1. Generic representation of the Multos card architecture

The application installation and deletion mechanism proposed by the Multos specification has a stringent and centralised architecture [18]. Every time an application is to be installed, an application provider will request an Application Load Certificate from the Multos Certification Authority through the appropriate card issuer. Because it has such a stringent architecture Multos is not considered the industry's leading architecture. This title goes to the Java Card technology, which has proliferated in the smart card industry because of its flexibility and robustness, and its readily available pool of experienced developers.

2) Java Card: It has progressed from the initial release which supported only limited functionality (i.e. primitive data types such as Boolean, byte and short) to the more recently released Java Card specification 3.0 [11] which includes the TCP/IP stack [19] along with SSL/TLS [20] and HTTP [21] /HTTPS [11], [22], [23]. The Java Card can behave as an internet device in either a server or client capacity. The

[1]Information Technology Security Evaluation Criteria (ITSEC) is an international security assurance evaluation criteria [14].

architecture of a Java Card is illustrated in Figure 2 and is described below:

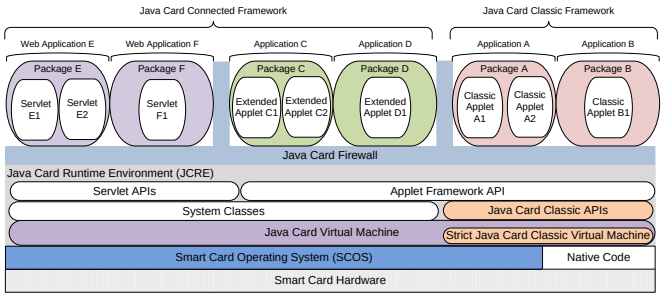

Fig. 2. Generic representation of the Java Card 3 architecture

In comparison to Multos, Java Card is better termed a platform rather than an operating system. Due to this distinction, above the smart card hardware layer, a native operating system is placed that is developed by each card manufacturer to support its implementation of the Java Card Virtual Machine (JCVM). Furthermore, as Java-based code might take longer to execute than the native code, the native method segment is the crucial point for implementing the cryptographic algorithms. Above this layer, we have the Java Card Runtime Environment (JCRE), which provides different services in the shape of Application Programming Interfaces (APIs) and System Classes to the residing applications. The Java Card APIs provide a well-structured framework to access the system-level services in a secure and reliable manner. The segregation on a Java Card between platform-application and application-application is enforced by the Java Card firewall.

The Java Card specification leaves decisions regarding the mechanism for installing, deleting, updating, and managing multiple applications on a smart card to the card manufacturer. The industry appreciated this move, as it allowed greater flexibility than Multos, which is rigid in comparison. However, it was soon realised that for application management tasks it would be beneficial for all the players in the smart card industry to have a unified specification. The proposed application management framework came in the form of the GlobalPlatform card specification, which is the topic of the next section.

3) GlobalPlatform: Towards the end of the 1990s, smart card technology was being adopted on a large scale. It was soon realised by card manufacturers, card issuers, and application providers that to manage such a complex and technically complicated infrastructure, it would be beneficial to share a unified and universal card management system which freed them from the demands of the smart card hardware, platform, application service and card issuer's requirements. Visa gave the impetus to this idea by transferring their Open Platform initiative to a consortium of card issuers, application providers, and smart card manufacturers, later known as GlobalPlatform.

The GlobalPlatform card specification is a card architecture-neutral specification which does not require/specify any particular Runtime Environment (RTE). However, at present most smart cards which support the GlobalPlatform specifications actually call for a Java Card Runtime Environment (JCRE).

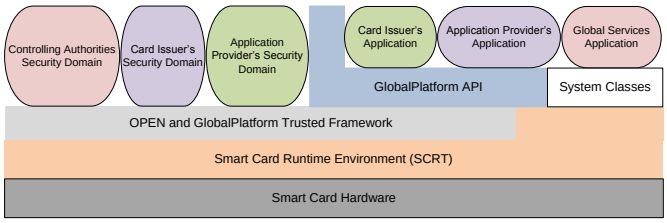

Fig. 3. Generic representation of the GlobalPlatform card architecture

The architecture illustrated in Figure 3 has applications from the card issuer, application providers (partners of the card issuer) and a global service application, which provides services to all the applications installed on the smart card. The applications are managed and controlled by the mechanism of security domains. A security domain has an association with one of the application(s) via which it manages and enforces the security policies of the owner of the domain. The security domain also provides separate cryptographic keys to the card issuer and the application providers to permit management of their respective domains/applications. The security domain also manages key handling, encryption, decryption, digital signature, and the verification of (hosted) applications (i.e. only at the time of installation [13], [24]). The card issuer generates the security domain (application domain) on the card and then gives control of the application domains to the card issuer's partners (application providers). These application providers can then manage their applications independently of the card issuer's involvement.

The OPEN framework defined in the GlobalPlatform specification handles/controls the downloading and installation of applications. The Trusted framework enables different services such as inter-application communications; however, the "GlobalPlatform Card Security Requirement Specification" [25] states that GlobalPlatform relies on the underlying platform's (e.g. Java Card) implementation of the firewall mechanism.

The crucial component of the GlobalPlatform card specification is termed the Card Manager. This is a generic term used for such services as OPEN, the issuer security domain and Cardholder verification method services. The Card Manager actively controls the smart card environment. Furthermore, the smart card issuer cannot access any of the application domains because they are protected by the cryptographic keys (access keys) and these keys are shared only between an application domain and an application provider. However, if a particular application provider violates the agreement with the card issuer, or they no longer have a partnership to provide services, then the card issuer can block or delete the application provider's application.

III. Security Models for Multiapplication Smart Cards

This section discusses different security models that have been proposed for smart card deployments [26].

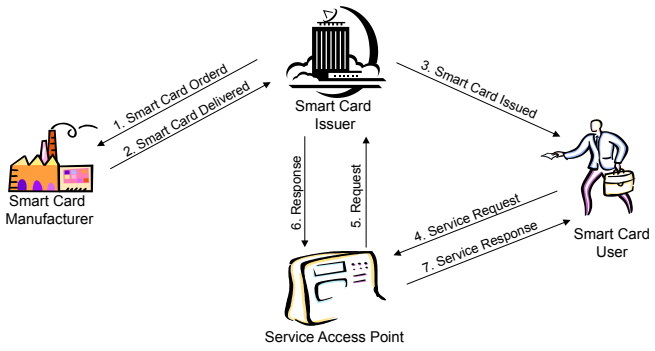

Fig. 4. Overview of the Issuer Centric Smart Card Ownership Model (ICOM)

A. Issuer Centric Smart Card Ownership Model

In Figure 4, smart card issuers are companies (e.g. in the banking, transport and telecom sectors), which use smart cards to provide services to their customers. The card issuers order smart cards from a card manufacturer. The card manufacturer delivers them to the card issuer or in some cases posts the ordered smart cards directly to the users (on behalf of the respective card issuer), which in turn issues them to individual cardholders. A cardholder presents her smart card at a Service Access Point (SAP) to use the services provided by the card issuer. A SAP can be an ATM (Automated Teller Machine), a mobile phone or a simple card reader; it acts as a gateway to a card issuer's services.

In this framework, the control of the issued smart cards lies with the card issuer, who decides what application(s) will be installed on the cards. If a card issuer has a business agreement with any other company, then the cardholder may get a smart card with multiple applications, as in the case of the Barclaycard's OnePulse card [27]. Barclaycard[2] is the card issuer and it has an established business relationship with Transport for London[3] (issuer of Oyster cards [28]). Therefore, with its bankcard, Barclays provides the Oyster card functionality.

The ICOM requires a trusted centralised authority to be set up which will have supervisory authority over smart cards. This centralised authority can be either the card issuer or a certifying authority. For convenience, we use the term card issuer to refer to any centralised authority in regard to the ICOM. The role of the authority is to enforce the security policy, which enables all the applications on a smart card to behave in a predefined manner. The predefined manner is negotiated between the application provider concerned and the card issuer. This agreement defines the parameters under which the application provider may access different services on the card issuer's smart cards. Furthermore, the card issuer will have the authority to grant or deny access to any particular application provider.

[2]Barclaycard: Barclaycard is a trading name for the banking card sector of Barclays Bank PLC, United Kingdom.

[3]Transport for London (TfL) is a publicly owned company that provides transport services to Greater London, United Kingdom.

Smart cards in the ICOM are acquired by the card issuer, which is in a position to choose their operational and security functionality. This gives assurance to the purchasing company (the card issuer) that the smart cards that carry its applications are secure to their required standard. If the card issuer required a third party evaluation of the smart card product, the card manufacturer might provide the Common Criteria [17] evaluation certificate (a paper based certificate) as a means of assurance.

To summarise the ICOM framework, the privileges or rights that a card issuer receives as part of the ICOM are listed below:

1) Privilege to install an application.
2) Privilege to delete an application.
3) Control over card issuance to individual users. This enables the issuers to decide who receives their smart cards (and effectively control their application).
4) Power to define the security and operational requirements for the smart cards.
5) Enforcement of the security policy.
6) Control over who can access their services using the issued smart cards.

The security and operational assumptions discussed above are the cornerstones of the ICOM.

B. Certificate Based

In this model, a third party will have the oversight of the smart card's security policy that both the card issuer (e.g. SP) and application providers have to abide by.

C. Open Card

In this approach, the customers would take the role of card issuer and acquire (blank) smart cards from a card manufacturer. A customer would then acquire an application from an organisation (e.g. bank, telecom and transport, etc.) and install this onto his or her smart card. This approach was not considered a serious contender as organisations may not trust the customer and might not have behaviour guarantees on the smart card platform.

D. Who took the Day?

Smart cards are traditionally deployed in inherently insecure environments with the strong assumption that their users might have malign intent. In such an environment, multiapplication smart cards with applications from different application providers (i.e. SPs) prompted debate over which security policy (discussed above) should be adopted.

As noted by M'Chirgui [2], the smart card industry's rapid proliferation was due to the adoption of the coopetition attitude towards the product and market; as noted for other high-tech industries. The concept of coopetition can be described as two individuals (companies) who cooperate with each other to cook a pie (establish a market) and then they compete with each other to take the biggest share of it. Examples of coopetition include EMV [6], GlobalPlatform [13], and Java Card [11] specification. However, a similar attitude was not apparent for the deployment of the multiapplication smart card initiative

for a diverse set of reasons. Following are a few of the major issues that contributed to the deceleration of the convergence of diverse services on a single device.

1) Smart Card Control (Ownership)
2) Marketing Potential
3) Customer Loyalty
4) Customer Relationship Management
5) Potential Revenue Source

The above-mentioned reasons may overly simplify the dynamics that led to the deceleration of the multiapplication smart card initiative. Nevertheless they played their role, and recently these issues have returned, as the concept of having multiapplication applications on a single device is gaining momentum.

IV. Current Trends in Multiapplication Smart Cards

In recent years, the smart card industry has trialled different approaches to the deployment of smart card-based services using mobile handsets. This section discusses the Near Field Communication technology and associated deployment architecture referred to as Trusted Services Manager (TSM).

A. Near Field Communication

The most important innovation that has influenced smart card technology in recent years is Near Field Communication (NFC), which enables a mobile phone to emulate a contact-less smart card [29]. This allows NFC-enabled mobile phones to perform contact-less card transaction on the existing smart card infrastructure (i.e., contact-less smart card terminals [1]). Therefore, it does not require any modification on the infrastructure side of the smart card service ecosystem. The only change is that a user's mobile phone acts as a contact-less smart card and from terminal's point of reference it communicates on a contact-less interface with a device that can be a traditional smart card or a mobile phone. The NFC trails are being carried out in 38 countries around the world [30].

In addition to the developments taking place in terms of NFC and its implications for the traditional smart card industry, smart card users cannot be isolated from the concept referred to as the "iPhone effect". Installing an application onto a mobile was possible even before the iPhone came to market. However, the iPhone made it consumer-friendly; an average customer can easily navigate, search, and install third party software [31]. In addition, the application developers do not have to negotiate with the mobile operators to download their applications onto the iPhone. Furthermore, Apple has managed to remain in the sales loop by charging a percentage on application sales directly to the application developers. Finally, mobile operators got the opportunity to sell data plans and generate revenue from the data usage.

With a growing and ever-younger consumer base that uses mobile phones for a multitude of purposes [32], it is obvious that the smart card service sector could also harness the platform to reduce their investment (i.e. purchasing of new smart cards), decrease roll-out time for new services, and remain competitive. An example of the competitive challenge faced by the traditional smart card industry is mobile payment systems; there are a number of smart phone Apps (i.e. Starbucks Apps for Blackberry and iPhone, and PayPal App, etc.) that a user can download onto their mobile phones and then can use them to pay for different services.

The multiapplication smart card initiative has matured to a level where it can be considered as a secure, reliable and viable platform. The convergence of different services on to a single device might be considered a natural next step in smart card evolution. However, how successful this might be is still open to debate. The next section discusses the proposed (and trialled) business models for the NFC based services roll-out.

B. Trusted Service Manager (TSM)

A Trusted Service Manager (TSM) is an entity that manages the collaborative architecture in which different application providers share a platform[4]. The TSM can be a card issuer or a third party to whom the card management tasks [33], [34] are being delegated by the scheme participants (e.g. card issuer and application providers). In current proposals a TSM can be: a) a Mobile Network Operation (MNO) [34], [35], b) a Card Issuing Bank (CIS) [36], [37] or c) A neutral third party.

No matter who takes the role of the TSM in a particular roll out, an ownership architecture has to be decided among the scheme participants. Some of the possible architectures listed in the literature [33]–[35], [38]–[40] are described in the subsequent sections.

1) Hotel Architecture: In this architecture, the card issuer owns the smart cards and either it can act as a TSM to control and manage the architecture or give it to a neutral third party. The TSM whose role is to control and manage the spaces (i.e. can be considered as rooms in a hotel); issues them to any requesting application providers. The lease of individual spaces can be time/space dependent. The application providers can access their spaces and utilise them according to the terms and conditions set by the TSM. The TSM will also have access to individual spaces; so it means that the keys that are used to manage individual spaces in the scheme are with an application provider that is using that space and the TSM. The maintenance of individual spaces can be managed by the TSM and might also include managing the customer relations of the individual application providers.

This architecture is stringent in terms of what an application provider can and cannot do with the allocated space. The scheme manager (i.e. TSM) can evict any application provider from the smart card, along with having the right to access these spaces.

[4]Platform: The term platform in context of the TSM refers to the secure elements present in a mobile phone. Secure elements can be Universal Integrated Circuit (UICC), embedded secure element, and Secure Memory Card [33].

2) Rental Architecture: This model is similar to the hotel architecture in many aspects, but the main difference is that the TSM issues a lease to application providers and this lease assigns the space on the smart card along with cryptographic keys to manage it. The TSM has access to these keys and they will be independently managed by the individual application providers. The TSM still has the authority to evict any application from the smart card but they do not have the right to access the memory space allocated to individual application providers. The lease in rental architecture is also time/space dependent but usually it is longer than the one issued in a hotel architecture.

The maintenance of individual spaces is delegated to individual application providers. In addition, in individual leases can have different sets of rules and regulations depending upon the TSM and respective application providers discretion. This architecture gives control of the smart card space to individual application providers.

3) Permanent Ownership Architecture: Individual spaces are permanently owned by scheme participants. Its similar to a building comprised of flats that are individually owned by the residents. There is a set of rules and regulations that are agreed among the scheme participants. As long as individual application providers abide by these rules and regulations they can utilise the space that they own. For security, reliability, and operational management the scheme participants can either choose one entity among themselves or hire a third party. The entity that would perform these duties is designated the TSM.

In this scheme no single entity can evict other entity, unless that entity has broken the agreed rules and regulations, and all other participants agree in principle.

V. Possible Future Direction for Multiapplication Smart Cards

This section discusses proposals for the future of smart card technology.

A. GlobalPlatform Consumer-Centric Smart Cards

This model enables users to acquire a secure token (e.g. smart card) from any provider (e.g card manufacturer and/or card issuer) and then manage the device as they please [49]. The proposed model is based on the GlobalPlatform architecture with the application installation/deletion privilege given to the users via a token provider. The proposed new model is similar to the User Centric Smart Card Ownership Model (UCOM) [41]. Therefore, instead of detailing the GlobalPlatform model, the UCOM is described in the next section. In the rest of this paper, the term consumer/user centric smart card refers to GlobalPlatform Consumer-Centric and User Centric Smart Cards.

B. User Centric Smart Card Ownership Model (UCOM)

The architecture of the User Centric Smart Card Ownership Model (UCOM) supports smart card ownership being with the cards user. The term ownership does not imply that the cardholder owns the platform as a card issuer would in the ICOM or TSM architectures. It implies that the user has the "*freedom of choice*" [41] to install or delete any application they require on their smart card. The card issuers or application providers in the ICOM or TSM architecture are termed Service Providers in the UCOM. A Service Provider (SP) is an organisation that will develop a smart card-based application and then issue its customers with unique credentials to download its application(s) directly to their respective smart cards [42].

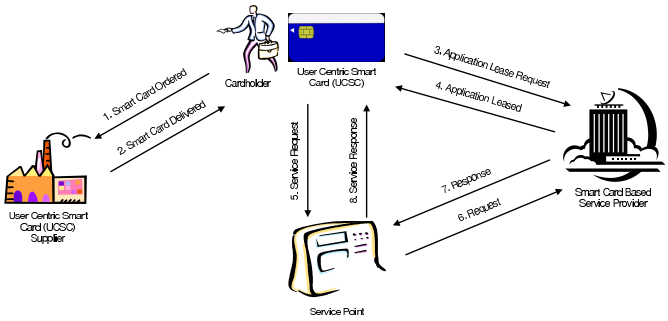

Fig. 5. Generic Overview of User Centric Smart Card Model (UCOM)

As shown in Figure 6, a card issuer acquires a UCOM-supported smart card referred as a User Centric Smart Card (UCSC) from a card manufacturer. At this stage, the card might be a blank card under default ownership. The default ownership means that its under the ownership of the card manufacturer. The cardholder initiates ownership transfer to him or herself and then can present this card to a SP to request their applications. The SP would decide the lease of the applications depending upon their Application Lease Policy (ALP) [42] which basically states the minimum security and operation requirements a smart card has to meet to get the lease. Only after the smart card satisfies the lease requirement of the SP [43], can the application be downloaded onto it. The cardholder is not involved in this process except for initiating the request for the application lease.

1) Why User Centric Smart Card Ownership: UCOM architecture is different from the Open Card initiative [45], multi-functional smart card [5] or virtual smart card (applications) [46]. The UCOM is in fact an ownership model rather than a complete platform or smart card operating system. To support UCOM requirements and services [41], the existing well-defined and studied architectures (e.g. Java Card [11], Multos [12], and GlobalPlatform [13]) are being modified [47] so they can efficiently support the user's ownership. Therefore, the main ingredients to support a user's ownership in a secure, reliable, flexible and ubiquitous way are already there. The only thing UCOM has done is to bring them together to support the concept of user-owned security devices (namely smart cards or secure element). The argument that an SP has to trust a cardholder before issuing its application is not valid [43] as the application lease is under the sole discretion of the respective SP. In addition, only after gaining assurance and validation that the smart card in question supports its requirements will it lease the application [44]. Therefore, the SP has to establish trust in the user's smart card and not

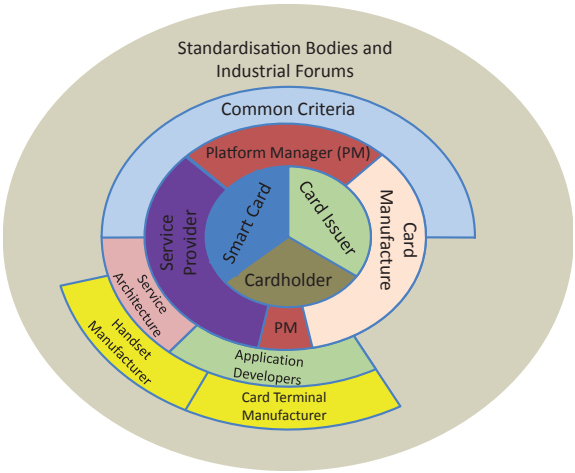

Fig. 6. Coopetitive Architecture's Smart Card Ecosystem

the user. It is the smart card that has to provide security and reliability assurance; whereas, the respective user can have malign intentions. A valid argument can be made that the UCOM architecture will only bring more complexity or complicate the security-sensitive smart card industry. It is true that the UCOM proposals do require some modification to the existing smart card platform but not to the services architecture (i.e. ATMs in banking, or turnstile terminal for transport services) .

C. Coopetitive Smart Cards

The ecosystem of a coopetitive architecture is illustrated in Figure 6. At its centre there are three main entities; smart card issuer, cardholder and smart card. The card issuer (or TSM) would issue smart cards to its respective customers. As a card issuer they would have their application pre-installed on to the smart card. The cardholder would have the choice to install or delete any application they require, except for the card issuer's application(s). The management of the smart card application installation, deletion, and application/card lifecyle is handled by the Platform Manager (PM). It helps both the card issuer and the cardholder to perform their sanctioned tasks.

As an example, consider a scenario in which a user enrols into the multiapplication smart card service architecture through a Mobile Network Operator (MNO). As a customer of the MNO, the user can receive an NFC-enabled mobile phone (under a fixed period contract) and secure element(s) that support multiapplication architecture. As per current architecture, the MNO subsidises the mobile phone in return for a fixed-period contract with its customers. The phone is under MNO lock and it can only be used on the issuing MNO's network. At the end of the contract, the customer can request the relevant MNO to unlock the mobile phone. The acquired secure element(s) would have the MNO's application installed by default. In addition, if the user is a customer of any other organisations that are associated partners with the MNO in the TSM scheme, then he or she may get their applications pre-installed on the secure element. The issuer secure element would enable the user to request installation or deletion of any application he or she requires, except for the MNO's application. At the end of the contract the MNO would not only unlock the mobile phone but also the TSM. From this point forward, the user can either use the secure element under UCOM architecture or register their secure element with any other TSM (or continue with the original MNO).

Similarly, other entities like banks, transport operators, smart card and mobile phone manufacturers, or independent third parties can participate by offering competitive products that adhere to the coopetitive architecture. The security and reliability of the coopetitive smart cards would be a key issue which is dealt with separately in the ICOM and UCOM scenarios. However, it is likely that further work would only strength the contribution that an open and dynamic system can bring to the multiapplication smart card architecture.

The fundamental attributes of the coopetitive architecture for multiapplication smart cards are listed below.

1) The scheme manager (TSM) would enable the provision for cardholders to request installation or deletion of any applications as they require.
2) To provide privacy to the cardholders, the applications that they request to install or delete would not be revealed to the respective TSM, unless the application in question is from an associate of the TSM. In that case the TSM would be notified of installation and deletion. For any independent entity (not related to the respective TSM), the identity of the application would be revealed to the TSM.
3) The security and reliability of the platform has to be decentralised. In scenarios where a cardholder does not want to reveal who is the active TSM of the card, the relevant smart card would still be able to provide security assurance and validations in an unlinkable way. The unlinkability relates to a mechanism that does not rely on the TSM, but on an independent third party's evaluation (i.e. Common Criteria Evaluations [17], [43], [44]). The property of the unlinkability would be that application providers that did not belong to the respective TSM would not know whether the requesting user was with a particular TSM or not. Similarly, the TSM should not know whose application is being requested to be installed or deleted from the secure element.
4) The cardholder should be given the choice to change the TSM if they require after meeting the terms and conditions of the original TSM. This would enable cardholders to move to TSMs that they consider provide them with the best service. Obviously, the original TSM has made an investment in the platform that is issued to the cardholder. Therefore, a cardholder would have to honour any terms and conditions that he or she agreed to at the time of acquiring the secure element.
5) If a cardholder does not want to be with any of the TSMs, then the framework should move back to default UCOM architectures. Similarly, the TSMs would also have the choice to remove the privileges of a cardholder

to install or delete applications, if the cardholder does not conform to the TSM's terms and conditions.

D. User Centric Tamper-Resistant Device

The motivation for having a generic tamper-resistant device that is under the control of its user rather than a centralised authority comes from three distinct but interrelated computing fields: smart cards, mobile platforms, and traditional Personal Computers. The User Centric Tamper-Resistant Device (UCTD) provides an underlying architecture that is secure, reliable, and flexible across different computing domains. A user can use her UCTD as a smart card device, and to secure her applications/communications on her mobile device and/or laptop. This proposal combines the security and privacy-preserving architecture across three computing fields with a single device architecture.

The multiapplication smart card architecture has the potential to serve as the underlying framework for the UCTD. The crucial point that has to be taken into account is that smart card architecture is traditionally under stringent centralised control, whereas the UCTD requires a more diverse architecture which also accommodates the user's ownership. Therefore, the concept of the User Centric Smart Card Ownership Model (UCOM) becomes synonymous with the UCTD. In addition to the UCOM framework for smart cards, for the UCTD initiative the form factor of smart cards is also diversified as shown in Figure 7.

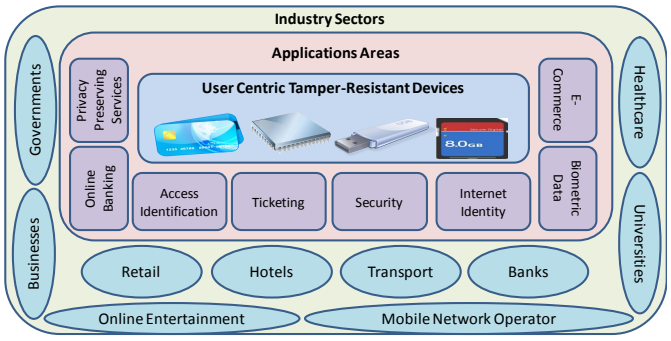

Fig. 7. Illustration of UCTD form factors, application areas, and industry sectors

E. Technical Challenges

By opening up the smart card platform, the traditional security architecture might not remain valid. For this reason, the smart card platform has to be improved to keep up with developments in associated computing environments.

Features like multi-threading, Web servers for smart cards, and high speed I/O will no doubt make smart card technology the generic security device of the future but this also poses new security challenges. The future smart card architecture has to implement effective execution time bytecode verification. In addition, an advance runtime protection mechanism is necessary to avoid faults and/or combined attacks.

The smart cards of the future, if they take the path of consumer-centric or user-centric smart cards, would require on-demand security evaluation and validation mechanisms. These mechanisms will enable the application providers to verify that the smart card is secure for their respective applications. The smart card firewall mechanism (application sharing mechanism) also requires refinement to cope with the dynamic nature of future smart cards - having a robust design to avoid feature interaction problems. The application installation and deletion process has to be redesigned to bring it in line with the dynamic nature of the future proposals for smart card technology.

F. Business Challenges

The FIPR (Foundation for Information Policy Research) published a white paper [48] in 1999, putting forward the notion that multiapplication smart cards are a bad idea. One of the big issues was the management of individual applications, independent of the control of the card issuer. In addition, there was the problem of what would happen if one of the applications on a multiapplication smart card was insecure — making the whole platform insecure. Since then, smart card technology has come a long way. However, business issues still need to be sorted out before TSM or consumer/user centric smart cards can become a reality. These business issues are related to the point discussed in section III-D. TSM and consumer/user centric models are trying to address these business issues but the uptake is slow. Once the TSM architecture matures and is deployed to a substantial mass, it will pave the way for the consumer/user centric models.

VI. Conclusion

Smart card technology has come a long way from a monoapplication platform to the present multi-threading environment. The wide-scale adoption of smart card technology is evidence of its merit. The technology has matured to a point where it has the ability to break out of the traditional applications and become a cross-computing platform security and privacy-preserving device. To reach this goal, substantial improvements and modifications are required but it seems that smart card technology has what it takes to be a de-facto security and privacy-preserving device for a diverse range of applications running on heterogeneous platforms.

References

[1] K. Mayes and K. Markantonakis, Eds., *Smart Cards, Tokens, Security and Applications*. Springer, 2008.

[2] M' Chirgui, Zouhaier, "The Economics of the Smart Card Industry: Towards Coopetitive Strategies," *Economics of Innovation and New Technology*, vol. 14, no. 6, pp. 455–477, 2005.

[3] J.-J. Quisquater, "The Adolescence of Smart Cards," *Future Generation Computer Systems*, vol. 13, no. 1, pp. 3 – 7, 1997.

[4] W. Rankl and W. Effing, *Smart Card Handbook*, 3rd ed. New York, NY, USA: John Wiley & Sons, Inc., 2003.

[5] D. Sauveron, "Multiapplication Smart Card: Towards an Open Smart Card?" *Inf. Secur. Tech. Rep.*, vol. 14, no. 2, pp. 70–78, 2009.

[6] *EMV 4.2*, Online, EMVCo Specification 4.2, May 2008. [Online]. Available: http://www.emvco.com/specifications.aspx?id=155

[7] W. Atkins, *The Smart Card Report*, 8th ed. Elsevier, January 2004.

[8] E. Brack, "Electronic Wallet Development Determinants: Theoretical and Empirical Analysis: Moneo," University Library of Munich, Germany, MPRA Paper 23453, 2003.

[9] D. Deville, A. Galland, G. Grimaud, and S. Jean, "Smart Card Operating Systems: Past, Present and Future," in *In Proceedings of the 5 th NORDU/USENIX Conference*, 2003.

[10] K. Markantonakis, "The Case for a Secure Multi-Application Smart Card Operating System," in *ISW '97: Proceedings of the First International Workshop on Information Security*. London, UK: Springer-Verlag, 1998, pp. 188–197.

[11] *Java Card Platform Specification*, Oracle Std. Version 3.0.1, May 2009.

[12] *Multos: The Multos Specification,*, Online, Std. [Online]. Available: http://www.multos.com/

[13] *GlobalPlatform: GlobalPlatform Card Specification, Version 2.2,*, GlobalPlatform Std., March 2006.

[14] "Information Technology Security Evaluation Criteria (ITSEC) - Provisional Harmonised Criteria," Office for Official Publications of the European Communities, Brussels, COM(90) 314, June 1991.

[15] "Multos: Version 4 on Hitachi AE45C Integrated Circuit Card," Uk IT Security Evaluation and Certification Scheme, Cheltenham, United Kingdom, Certification Report NO. P167, June 2002.

[16] T. Frane-Massey, "Multos - the High Security Smart Card OS," MAOSCO, Tech. Rep., September 2005.

[17] *Common Criteria for Information Technology Security Evaluation*, Common Criteria Std. Version 3.1, August 2006.

[18] "Multos: Guide to Loading and Deleting Applications," MAOSCO, Tech. Rep. MAO-DOC-TEC-008 v2.21, 2006.

[19] "RFC 1122 - Requirements for Internet Hosts - Communication Layers," United States, Tech. Rep., 1989.

[20] T. Dierks and E. Rescorla, "RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2," Tech. Rep., August 2008.

[21] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "RFC 2616 - Hypertext Transfer Protocol – HTTP/1.1," United States, Tech. Rep., 1999.

[22] E. Rescorla and A. Schiffman, "RFC 2660 - The Secure HyperText Transfer Protocol," United States, Tech. Rep., 1999.

[23] *Smartcard-Web-Server, Smartcard Web Server Enabler Architecture, Smartcard Web Server Requirements*, Open Mobile Alliance (OMA) Std., 2008.

[24] K. Markantonakis and K. Mayes, "An Overview of the GlobalPlatform Smart Card Specification," *Information Security Technical Report*, vol. 8, no. 1, pp. 17 – 29, 2003.

[25] "GlobalPlatform Card Security Requirement Specification 1.0," Online, Redwood City, USA, Specification, May 2003.

[26] P. Girard, "Which Security Policy for Multiplication Smart Cards?" in *the USENIX Workshop on Smartcard Technology*. USA: USENIX Association, 1999, pp. 3–3.

[27] Barclaycard OnePulse. BarclayCard, Barclay Bank PLC. UK.

[28] London Underground: Oyster Card. London Underground. UK.

[29] *ISO/IEC 18092: Near Field Communication - Interface and Protocol (NFCIP-1)*, ISO Std., April 2004.

[30] NFC Trials, Pilots, Tests and Live Services around the World. Online. NFC World.

[31] J. Laugesen and Y. Yuan, "What Factors Contributed to the Success of Apple's iPhone?" in *Proceedings of the 2010 Ninth International Conference on Mobile Business*, ser. ICMB-GMR '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 91–99.

[32] "The Apple iPhone: Success and Challenges for the Mobile Industry," Online, Rubicon Consulting Inc., USA, Tech. Rep., March 2008.

[33] "The GlobalPlatform Proposition for NFC Mobile: Secure Element Management and Messaging," GlobalPlatform, April 2009.

[34] J. Guaus, L. Kanniainen, P. Koistinen, P. Laaksonen, K. Murphy, J. Remes, N. Taylor, and O. Welin, "Best Practice for Mobile Financial Services: Enrolment Business Model Analysis," Mobey Forum Mobile Financial Services Ltd., Helsinki, Finland, Online, June 2008.

[35] "Mobile NFC Services," GSM Association, White Paper V1.0, 2007.

[36] "EMV Mobile Contactless Payment: Technical issues and Position Paper," Online, EMVCo., California, USA, Tech. Rep., October 2007.

[37] "The Role and Scope of EMVCo in Standardising the Mobile Payments Infrastructure," Online, EMVCo., USA, Tech. Rep., October 2007.

[38] G. Madlmayr, J. Langer, and J. Scharinger, "Managing an NFC Ecosystem," in *ICMB '08: Proceedings of the 2008 7th International Conference on Mobile Business*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 95–101.

[39] "Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications," White Paper, November 2006.

[40] "Pay-Buy-Mobile: Business Opportunity Analysis," GSM Association, White Paper 1.0, November 2007.

[41] R. N. Akram, K. Markantonakis, and K. Mayes, "A Paradigm Shift in Smart Card Ownership Model," in *the 2010 International Conference on Computational Science and Its Applications (ICCSA 2010)*, B. O. Apduhan, O. Gervasi, A. Iglesias, D. Taniar, and M. Gavrilova, Eds. Japan: IEEE CS, March 2010, pp. 191–200.

[42] ——, "Application Management Framework in User Centric Smart Card Ownership Model," in *The 10th International Workshop on Information Security Applications (WISA09)*, H. Y. YOUM and M. Yung, Eds., vol. 5932/2009. Busan, Korea: Springer, August 2009, pp. 20–35.

[43] ——, "A Dynamic and Ubiquitous Smart Card Security Assurance and Validation Mechanism," in *25th IFIP International Information Security Conference (SEC 2010)*, ser. IFIP AICT Series, K. Rannenberg and V. Varadharajan, Eds. Aus: Springer, September 2010, pp. 161–172.

[44] ——, "Simulator Problem in User Centric Smart Card Ownership Model," in *6th IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom-10)*, H. Y. Tang and X. Fu, Eds. HongKong, China: IEEE Computer Society, December 2010.

[45] S. Chaumette and D. Sauveron, "New Security Problems Raised by Open Multiapplication Smart Cards." *LaBRI, Université Bordeaux 1.*, pp. 1332–04, 2004.

[46] R. N. Akram, K. Markantonakis, and K. Mayes, "Location Based Application Availability," in *On the Move to Meaningful Internet Systems: OTM 2009 Workshops*, R. M. P. Herrero and T. Dillon, Eds., vol. 5872/2009. Portugal: Springer, November 2009, pp. 128 – 138.

[47] ——, "Firewall Mechanism in a User Centric Smart Card Ownership Model," in *Smart Card Research and Advanced Application, 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010*, D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, Eds., vol. 6035/2010. Passau, Germany: Springer, April 2010, pp. 118–132.

[48] "Framework for Smart card Use in Government," Foundation for Information Policy Research, Consultation Response, 1999.

[49] A New Model: The Consumer-Centirc Model and How it Applies to the Mobile Ecosystem GlobalPlatform, 2012